

Notice of Allowability

Application No.

10/010,352

Examiner

Pramila Parthasarathy

Applicant(s)

SHELEST ET AL.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 7/13/2006.
2. ☒ The allowed claim(s) is/are 1-11 and 13-17; Renumbered as 1-16.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.
2. Applicant's submission filed on May 30, 2006 has been entered and made of record.

Response to Arguments

3. Applicant's arguments filed 5/30/2006 with respect to pending claims have been fully considered and are persuasive in view of the interview held on May 17, 2006 and the affidavit filed on 7/13/2006.

Allowable Subject Matter

4. Claims 1 – 11 and 13 - 17 are allowed and renumbered as 1 – 16.

Art Unit: 2136

5. The following is an examiner's statement of reasons for allowance: The Admitted prior art Diffie et al. U.S. Patent Number RE: 36,946, discloses a method and apparatus for providing a secure wireless communication link between a mobile device and a base computing unit. The mobile sends a host certificate to the base along with a randomly chosen challenge value and a list of supported shared key algorithm. The base verifies the certificate, which is digitally signed by a trusted certificate authority. If the certificate is valid, the mobile verifies under the public key of the base the signature of the message. If the base signature is valid, the mobile sends encrypted random number and encrypted public key to the base. The base then verifies the mobile signature using the mobile public obtained by the mobile certificate. If the mobile signature is verified, the base decrypts encrypted public key and random number using its private key. The base then determines the session key and the mobile and the base may then enter a data transfer phase using the encrypted data, which is decrypted using the session key.

However, the admitted prior art does not disclose, teach or suggest, "creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device derived from a portion of a combination of a hash of the public key and a modifier, and a digital signature, the digital signature generated by hash value of data including the content data; and

making the authentication information available to the second computing device."

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

7. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a personal interview with James R. Banowsky, registration number 37,773, on May 17, 2006.

IN THE CLAIMS:

1. (Amended) A method for a first computing device to make authentication information available to a second computing device, the method comprising:

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device derived from a portion of a combination of a hash of the public key and a modifier, and a digital signature, the digital signature generated by hashing a network address and at least a portion of the content data with a private key corresponding to the public key of the first computing device; and

making the authentication information available to the second computing device.

2. (Amended) A computer-readable storage medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device, the method comprising:

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device derived from a portion of a combination of a hash of the public key and a modifier, and a digital signature, the digital signature generated by hashing a network address and at least a portion of the content data; and

making the authentication information available to the second computing device.

Art Unit: 2136

3. (Amended) A method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;

deriving a portion of a second network address from the public key of the first computing device by taking a portion of a value derived by hashing a combination of the public key and a modifier;

validating the digital signature using the public key of the first computing device;
and

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the digital signature is valid.

5. (Amended) A computer-readable storage medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device that has a node-

Art Unit: 2136

selectable portion from a portion of a hash of a composite of the public key and a modifier, and a digital signature;

deriving a node-selectable portion of a second network address by taking a portion of a hash of the public key of the first computing device;

validating the digital signature using the public key of the first computing device;

accepting the content data if the node-selectable portion of the second network address matches the node-selectable portion of the first network address and if the digital signature is valid; and

wherein the second computing device accesses the public key of the first computing device over an unsecure channel.

6. (Amended) A method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the method comprising:

hashing the public key;

comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion; and

when the portion do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing steps.

8. (Amended) A computer-readable storage medium containing instructions for performing a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the method comprising:

hashing the public key;

comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion; and

when the portion do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing steps.

11. (Amended) A method for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a modifier, a first network address of the first computing device, and a digital signature;

appending the modifier to the public key of the first computing device and deriving a portion of a second network address from combination of the public key of the first computing device and the modifier;

validating the digital signature by using the public key of the first computing device; and

caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from at least one of the content data and a hash value of data including the content data.

Art Unit: 2136

12. Cancelled.

17. (Amended) A computer-readable storage medium containing instructions for performing a method for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a modifier, a first network address of the first computing device, and a digital signature;

deriving a portion of a second network address from combination of the public key of the first computing device and the modifier;

validating the digital signature by using the public key of the first computing device; and

caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from at least one of the content data and a hash value of data including the content data.

21 – 22. Cancelled.

Art Unit: 2136

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

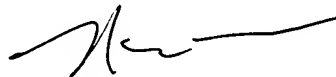
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
July 27, 2006.



NASSER MOAZZAMI
PRIMARY EXAMINER



07/28/06